COMBINED STATEMENTS OF

JAYSON P. AHERN
ASSISTANT COMMISSIONER, OFFICE OF FIELD OPERATIONS
U.S. CUSTOMS AND BORDER PROTECTION

AND

CAPTAIN BRIAN SALERNO
DEPUTY DIRECTOR, INSPECTIONS AND COMPLIANCE
UNITED STATES COAST GUARD

HEARING ON

"SAFE PORTS ACT"

BEFORE THE

SUBCOMMITTEE ON ECONOMIC SECURITY, INFRASTRUCTURE PROTECTION & CYBERSECURITY;

COMMITTEE ON HOUSE HOMELAND SECURITY

MARCH 16, 2006

I. Introduction and Overview

Chairman Lungren, Ranking Member Sanchez, Members of the Subcommittee, it is a privilege for the U.S. Coast Guard and U.S. Customs and Border Protection (CBP) to appear before you today to discuss the Department of Homeland Security's programs that are fundamental to securing our nation's ports, and maintaining the economic viability of the Marine Transportation System.

CBP, as the guardian of the Nation's borders, safeguards the homeland—foremost, by protecting the American public against terrorists and the instruments of terror; while at the same time, enforcing the laws of the United States and fostering the Nation's economic security through lawful travel and trade. Contributing to all this is CBP's time-honored duty of apprehending individuals attempting to enter the United States illegally, stemming the flow of illegal drugs and other contraband, protecting our agricultural and economic interests from harmful pests and diseases, protecting American businesses from theft of their intellectual property, regulating and facilitating international trade, collecting import duties, and enforcing U.S. trade laws. In FY 2005, CBP processed almost 29 million trade entries, collected $31.4 billion in revenue, seized 2 million pounds of narcotics, processed 431 million pedestrians and passengers, 121 million privately owned vehicles, and processed and cleared 25.3 million sea, rail and truck containers. We cannot protect against the entry of terrorists and the instruments of terror without performing all missions.

The Coast Guard is the Federal agency in charge of maritime security in our ports and waterways. The Coast Guard works very closely with other agencies to pursue a collective strategy of "layered security." Protective measures are implemented overseas within the global trade environment, others are implemented closer to our shores and then still other actions are taken within the U.S. ports themselves. In the overseas arena, the Coast Guard and CBP work together to identify security gaps in foreign ports through our International Port Security Program, which helps CBP position its resources appropriately to most effectively verify high risk cargo prior to loading onboard a ship bound for the U.S. Additionally, the Coast Guard has actively supported CBP on international delegations to develop international standards for supply chain security. The Coast Guard and CBP have also established mechanisms for CBP to obtain the cargo and crew information from the Coast Guard's electronic Advance Notice of Arrival system. This allows both agencies to conduct vessel screening and targeting operations for high risk vessels bound for the U.S. thereby increasing the layers of protection associated with these vessels before they reach our shores. The Coast Guard and CBP have exchanged liaison officers at CBP's National Targeting Center and at the Coast Guard's Intelligence Coordination Center to facilitate information sharing and operational response coordination when high risk cargo, vessels or crew are identified.

There are numerous other coordination initiatives underway that support cargo security.
The Coast Guard and CBP are working together both on program management and to plan for operational issues associated with "Operation Safe Commerce" project, the DHS container seal regulation project, and both national and local level operational coordination issues to target vessels and respond to threats, among others.

The concept of "layers of security" is complex, involving multiple types of activities to create a network of interdependent, overlapping and purposely redundant checkpoints designed to reduce vulnerabilities, as well as detect, deter and defeat threats. It entails developing security measures that cover the various components of the maritime transportation system, including people,

infrastructure, conveyances and information systems. These security measures span distances geographically—from foreign ports of embarkation, through transit zones, to U.S. ports of entry and beyond—and involve the different modes of transportation that feed the global supply chain; and are implemented by various commercial, regulatory, law enforcement, intelligence, diplomatic and military entities. A significant challenge to constructing integrated layers of security is the fact that many of the layers are the responsibility of different agencies. Integrating these disparate maritime security layers involves not only unity of effort, shared responsibility, partnership, and mutual support, but requires an agency with significant maritime security responsibilities to act as a coordinator for the purposes of integrating the government's efforts to provide layered security.

We must perform all missions without stifling the flow of legitimate trade and travel that is so important to our nation's economy. We have "twin goals:" Building more secure and more efficient borders.

II. **Meeting Our Twin Goals: Building More Secure and More Efficient Borders**

The Coast Guard works in concert with CBP to align respective agency roles and responsibilities regarding international trade. When cargo is moved on the waterborne leg of a trade route, the Coast Guard has oversight of the cargo's care and carriage on the vessels and within the port facility. The Coast Guard also oversees the training and identity verification of professional mariners who are transporting the cargo. CBP has authority over the cargo contents and container standards. Using the information provided through the Coast Guard's 96-hour notice of arrival rule and CBP's 24-Hour cargo loading rule, the Coast Guard and CBP act to control vessels (and their cargoes) that pose an unacceptable risk to our ports. As a further improvement, the trade community can file required passenger and crew information via an electronic notice of arrival and departure system. This streamlines the process for industry and improves our ability to apply targeting and selectivity methods. With Coast Guard officers posted at the NTC, we continuously improve agency coordination and our collective ability to quickly take appropriate action when notified of a cargo of interest.

As the single, unified border agency of the United States, CBP's missions are extraordinarily important to the protection of America and the American people. In the aftermath of the terrorist attacks of September 11th, CBP has developed initiatives to meet our twin goals of improving security and facilitating the flow of legitimate trade and travel. Our homeland strategy to secure and facilitate cargo moving to the United States is a layered defense approach built upon interrelated initiatives. They are: the 24-Hour and Trade Act rules, the Automated Targeting System (ATS), housed in CBP's National Targeting Center, the use of non-intrusive inspection equipment and radiation detection portal monitors, the Container Security Initiative (CSI), and the Customs-Trade Partnership Against Terrorism (C-TPAT).

Our remarks will focus primarily on how these complimentary layers enhance seaport security, and protect the nation.

Vessel Security

There are approximately 11,000 U.S. vessels that that require vessel security plans (6,200 inspected vessels and 4,800 un-inspected vessels). The Coast Guard received, reviewed and approved all domestic vessel security plans.

Since July 2004 the Coast Guard has conducted 16,000 foreign flag vessel boardings for security compliance with the International Ship and Port Security (ISPS) Code. These boardings were conducted either offshore or in port depending on the risk assessment completed prior to each vessel arrival in U.S port. From those 16,000 boardings the Coast Guard has imposed 143 detentions, expulsions or denials of entry for vessels that failed to comply with international security requirements.

In addition the Coast Guard has established a process to identify and target High Interest Vessels. This process has resulted in 3,400 at sea security boardings and 1,500 positive vessel control escorts since 2004 to ensure these vessels cannot be used as weapons of mass effect.

Advance Electronic Information

As a result of the 24-Hour rule and the Trade Act, CBP requires advance electronic information on all cargo shipments coming to the United States by land, air, and sea, so that we know who and what is coming before it arrives in the United States. 24-Hour Advanced Cargo Rule, requiring all sea carriers, with the exception of bulk carriers and approved break-bulk cargo, to provide proper cargo descriptions and valid consignee addresses 24 hours before cargo is loaded at the foreign port for shipment to the United States. However, bulk carriers are not exempt from all advance electronic information requirements – they are required to transmit cargo information 24 hours prior to arrival in the U.S. for voyages that exceed 24 hours sailing time from the foreign port of loading, or transmit at the time of departure to the U.S. for voyages less than 24 hours sailing time to the U.S. from the foreign port of loading. Failure to meet the 24-Hour Advanced Cargo Rule results in a "do not load" message and other penalties. This program gives CBP greater awareness of what is being loaded onto ships bound for the United States and the advance information enables CBP to evaluate the terrorist risk from sea containers on 100% of shipments.

In addition, the Coast Guard has taken multiple steps to enhance awareness in the maritime domain. One major step was the publication of the 96-hour Advanced Notice of Arrival regulations which requires vessels to provide detailed information to the Coast Guard 96-hours before a vessel arrives at a U.S. port from foreign ports. This regulation provides sufficient time to vet the crew, passengers, cargo and vessel information of all vessels prior to entering the U.S. from foreign ports By merging CBP and CG vessel and people information requirements into the electronic notice of arrival and departure, the reporting burden on the maritime industry will be reduced. Because the system was made available to the public on January 31, 2005, it afforded vessel owners and operators the time to become familiar with the electronic notice of arrival and departure, and consequently have an easier time complying with CBPs APIS regulation which mandated the use of this system by June 6, 2005, as the approved method for submission in accordance with the APIS regulation.

Automated Targeting System

The Automated Targeting System, which is used by National Targeting Center and field targeting units in the United States and overseas, is essential to our ability to target high-risk cargo and passengers entering the United States. ATS is the system through which we process advance manifest and passenger information to detect anomalies and "red flags," and determine which passengers and cargo are "high risk," and should be scrutinized at the port of entry, or in some cases, overseas.

ATS is a flexible, constantly evolving system that integrates enforcement and commercial databases. ATS analyzes electronic data related to individual shipments prior to arrival and ranks them in order of risk based on the application of algorithms and rules. The scores are divided into thresholds associated with further action by CBP, such as document review and inspection.

The National Targeting Center, working closely with the Coast Guard, also vets and risk scores all cargo and cruise-ship passengers and crew prior to arrival. This ensures that DHS has full port security awareness for international maritime activity.

Container Security Initiative (CSI) and Customs-Trade Partnership Against Terrorism (C-TPAT): Extending our Zone of Security Outward– Partnering with Other Countries

Every day, approximately 31,000 seagoing containers arrive at our nation's seaports equating to nearly 11.3 million a year. About 90% of the world's manufactured goods move by container, much of it stacked many stories high on huge transport ships. Each year, two hundred million cargo containers are transported between the world's seaports, constituting the most critical component of global trade.

All trading nations depend on containerized shipping. Of all incoming trade to the United States, nearly half arrives by ship, and much of that is in sea containers. Other countries are even more dependent on sea container traffic, such as the U.K., Japan and Singapore.

The fact is that, today, the greatest threat we face to global maritime security is the potential for terrorists to use the international maritime system to smuggle terrorist weapons – or even terrorist operatives – into a targeted country.

If even a single container were to be exploited by terrorists, the disruption to trade and national economies would be enormous. In May 2002, the Brookings Institution estimated that costs associated with United States port closures from a detonated terrorist weapon could amount to $1 trillion from the resulting economic slump and changes in our ability to trade.

Clearly, the risk to international maritime cargo demands a robust security strategy that can identify, prevent and deter threats, at the earliest point in the international supply chain, before arrival at the seaports of the targeted country. We must have a cohesive national cargo security strategy that better protects us against the threat posed by global terrorism without choking off the flow of legitimate trade, so important to our economic security, to our economy, and, to the global economy.

Our nation developed a cargo security strategy that addresses cargo moving from areas outside of the United States to our ports of entry. Our strategy focuses on stopping any shipment by terrorists before it reaches the United States, and only as a last resort, when it arrives at a port of entry.

The Container Security Initiative (CSI) and the Customs-Trade Partnership Against Terrorism (C-TPAT) initiatives bolster port security. The CSI initiative proposes a security regime to ensure that all containers posing a potential risk for terrorism are identified and inspected at foreign ports before they are placed on vessels destined for the United States. CBP continues to station multidisciplinary teams of U.S. officers from both CBP and Immigration and Customs Enforcement

to work together with our host foreign government counterparts to develop additional investigative leads related to the terrorist threat to cargo destined to the United States.

Through CSI, CBP works with host government Customs Services to examine high-risk maritime containerized cargo at foreign seaports, before they are loaded on board vessels destined for the United States. CSI is currently operational at 43 foreign ports. By the end of 2006, we expect that 50 ports, covering 82% of maritime containerized cargo shipped to the U.S., and by the end of 2007, we expect to be operational in 58 ports covering 85% of maritime containerized cargo destined to the United States.

As directed by MTSA, the International Port Security Program has begun visiting foreign countries to assess the effectiveness of anti-terrorism measures in foreign ports.

To date, 45 countries have been assessed; 40 have been found to be in substantial compliance with the International Ship and Port Facility Security (ISPS) Code. These 45 countries are responsible for over 80% of the vessel arrivals to the United States. The five countries that are not in substantial compliance have been or will soon be notified to take corrective actions or risk being placed on a Port Security Advisory and have Conditions of Entry imposed on vessels arriving from their ports.

The Coast Guard is on track to assess approximately 36 countries per year, with a goal of visiting all of our maritime trading partners within four years

Through C-TPAT, CBP establishes voluntary best security practices for all parts of the supply chain, making it more difficult for a terrorist or terrorist sympathizer to introduce a weapon into a container being sent by a legitimate party to the United States. C-TPAT covers a wide variety of security practices, from fences and lighting to requiring that member companies conduct background checks on their employees, maintain current employee lists, and require that employees display proper identification.

C-TPAT's criteria also address physical access controls, facility security, information technology security, container security, security awareness and training, personnel screening, and important business partner requirements. These business partner requirements oblige C-TPAT members to conduct business with other C-TPAT members who have committed to the same enhanced security requirements established by the C-TPAT program.

The C-TPAT program has created a public-private and international partnership with nearly 5,800 businesses (over 10,000 have applied), including most of the largest U.S. importers. Forth-five percent of all merchandise imported into the United States is done so by C-TPAT member importers. C-TPAT, CBP and partner companies are working together to improve baseline security standards for supply chain and container security. CBP reviews the security practices of not only the company shipping the goods, but also the companies that provided them with any services.

The validation process employed by CBP demonstrates and confirms the effectiveness, efficiency and accuracy of a C-TPAT certified member's supply chain security. At present, the C-TPAT program has completed validations on 27 percent (1,545 validations completed) of the certified membership, up from 8 percent (403 validations completed) a year ago. Additionally, validations are in progress on another 39 percent (2,262 in progress) of certified members, and these validations will be completed throughout 2006, bringing the total percentage of certified members

to 65 percent by years' end. In 2007, the C-TPAT program validations will continue. And we will have validated 100 percent by the end of CY 2007.

Additionally, CBP has moved to tighten minimum-security criteria for membership in this voluntary program. Working closely with the trade community and key stakeholders, CBP has developed and implemented baseline security standards for member importers, sea carriers, and highway carriers. CBP will complete this process by the end of CY 2006, defining the minimum-security criteria for the remaining enrollment sectors – air carriers, rail carriers, brokers, freight forwarders, and foreign manufacturers.

The Coast Guard supports several DHS initiatives such as Operation Safe Commerce (OSC), the Container Security Initiative (CSI) and the Customs-Trade Partnership against Terrorism (C-TPAT) to ensure mutual policies, programs and initiatives are complementary and cover the entire supply chain. The CSI and C-TPAT are programs that are designed to extend supply chain security improvements to overseas ports and further along the international supply chain.

Non-Intrusive Inspection Equipment and Radiation Detection Portals:

CBP also uses cutting-edge technology, including large-scale X-ray and gamma ray machines and radiation detection devices to screen cargo. Presently, CBP operates over 680 radiation portal monitors at our nation's ports, including 181 radiation portal monitors at seaports allowing us to scan 37 percent of arriving international cargo, and that number will continue to grow through the remainder of this year and 2007. CBP also utilizes over 170 large-scale non-intrusive inspection devices to examine cargo and has issued 12,400 hand-held radiation detection devices to its CBP officers.

Further, the DHS Domestic Nuclear Detection Office's (DNDO) FY 2007 budget request of nearly $536 million, a 70% increase from FY 2006, includes $157 million that will allow for the acquisition and deployment of nearly 300 current and next-generation radiation detection systems at our ports of entry. These funds, and funds provided in FY 2005 and FY 2006, will allow for the deployment of 621 RMPs to our Nation's top seaports, which will allow us to screen approximately 98 percent inbound containers by December 2007. These systems will be deployed and operated by CBP. In addition, DNDO's FY 2007 budget also includes $30.3 million for the development of enhanced cargo radiography screening systems for our ports of entry. These enhanced screening efforts will compliment the many information-based programs CBP already has in place for enhanced port security.

In addition to increased screening efforts at our own ports of entry for radioactive and nuclear materials, the Department fully endorses the concept of increased active and passive detection at foreign ports of departure. The systems DNDO is acquiring and developing can also be used by foreign ports with a CSI presence, as well as the Department of Energy's Megaports initiative. We must continue to stress the need for increased screening at foreign ports of departure while at the same time having a robust screening effort at our own ports of entry.

Port Security Grant Program and the Coast Guard

The Port Security Grant Program is administered by the Office of Grants & Training (OG&T) in the Preparedness Directorate of DHS. The Coast Guard continues to plays an active role in the Port

Security Grant Program, as it has in the first five rounds, and participates in the development of program guidance, conducts the field review process and is a member of the national review panel.

In round five of the Port Security Grant Program, $142 million was awarded for 132 projects. The current program has been improved substantially by using a risk-based formula to ensure that the projects funded provide the greatest risk reduction at the most critical ports. This same risk based formula will be used for round six in 2006.

Transportation Worker Identification Credential (TWIC)

The TWIC program, which will satisfy the requirements in MTSA under 46 U.S.C. § 47105, will ensure that only properly cleared and authorized personnel could gain access to secure areas of the Nation's transportation system.

The goals of the TWIC program are to:

- Develop a common, secure biometric credential and standards that are interoperable across transportation modes and compatible with existing independent access control systems;
- Establish processes to verify the identity of each TWIC applicant, complete a security threat assessment on the identified applicant, and positively link the issued credential to that applicant; and
- Quickly revoke card holder privileges for individuals who are issued a TWIC but are subsequently determined to pose a threat after issuance of their credentials, and immediately remove lost, stolen, or compromised cards from the system.

Encompassed within the TWIC program are requirements established by the Maritime Transportation Security Act of 2002 to prevent unaccompanied individuals from entering a secure area of a vessel or facility unless the individual holds a transportation security card. Additionally, the Act requires that all holders of Merchant Mariner Credentials obtain a TWIC. With MTSA as their guide, the Coast Guard and TSA have worked closely to develop the maritime component of TWIC and are currently preparing a joint Notice of Proposed Rulemaking (NPRM).

The Coast Guard is working very closely with the TSA to assist in the implementation of this new credentialing program. The Coast Guard is supportive of this regulatory effort. We will do everything within our ability to assist TSA in the development of this rulemaking and ensure that the TWIC and Merchant Mariner Credentialing initiatives are complementary in order to minimize the burden on mariners in the future.

Post TSI Coordination
National Response Options Matrix

The National Response Options Matrix (NROM) is intended to aid crisis action decision making at the national level, immediately following a maritime transportation security incident (TSI). It does not apply to the port experiencing the TSI, however. The NROM's goal is to provide senior leadership with immediate pre-planned short-term security options to prevent further attacks and protect the marine transportation system, maritime critical infrastructure and key assets (MCI/KA), and high density population centers, following a maritime TSI. NROM is a "Quick Reaction Card" decision aid for use by senior leadership to direct a possible Coast Guard wide security posture that may significantly impact maritime industry, change the maritime security (MARSEC) level, and

perhaps affect/involve other DHS agencies or departments. These options may include changes in MARSEC level (for Coast Guard forces and maritime industry), potential change(s) in Coast Guard force protection condition (FPCON), or other risk mitigation options on a national level, regionally, or by specific ports. NROM has scenario-based mitigation options that were designed to build upon and strengthen existing measures, surge resources as necessary, control or restrict certain port activity, and only if necessary, close ports. NROM could also be useful in evaluating the Coast Guard's response, if any, to U. S. or world-wide terrorist incidents outside of the maritime environment.

If a maritime TSI should occur in one of our ports, the local responders (Federal Maritime Security Coordinator (Coast Guard Sector or Captain of the Port), other Federal agencies, state and local authorities, and partners in industry) will immediately react with prevention, protection, mitigation, response, and recovery activities in that port and region. The premise of NROM is to have pre-planned security options that would be put in place in other ports throughout the country to prevent and protect against further attacks. The NROM is reflected in our planning for post-incident maritime infrastructure recovery activities under the National Strategy for Maritime Security that was approved by the President last year.

NROM answers the question, "What is being done in the other ports to prevent further attacks, protect maritime infrastructure and population centers, while facilitating the continued flow of commerce and legitimate use of the maritime environment." Currently, the Coast Guard is working with CBP to incorporate CBP's response/recovery measures, making it a joint-agency decision matrix document. We have also developed an electronic NROM to improve the visibility of the product and help facilitate its use.

III. Conclusion

In summary, as noted already, the Coast Guard, CBP, industry partners, and many other Federal, state and local agencies work hand in hand to screen cargo, the vessels that transport the cargo and the facilities that load and discharge cargo to mitigate the risk to the Marine Transportation System. All containers and vessels that CBP and the Coast Guard determine to be of risk are examined using a variety of technologies, either at the foreign port, at sea, or upon arrival into the U.S.

Mr. Chairman, Members of the Subcommittee, we have briefly addressed DHS's critical initiatives today that will help us protect America against terrorists and the instruments of terror, while at the same time enforcing the laws of the United States and fostering the Nation's economic security through lawful travel and trade. We realize there is more to do, and with the continued support of the President, and the Congress, DHS will succeed in meeting the challenges posed by the ongoing terrorist threat and the need to facilitate ever-increasing numbers of legitimate shipments and travelers.